**UNITED STATES DISTRICT COURT**
**DISTRICT OF MARYLAND**

PAMELA HUNTER, individually and on behalf of all others similarly situated,
752 Lannerton Rd
Middle River, MD 21220

Plaintiff,

v.

THE JOHNS HOPKINS UNIVERSITY
Charles & 34th Street
Baltimore, MD 21218

and

THE JOHNS HOPKINS HEALTH SYSTEM CORPORATION
600 N. Wolfe Street
Baltimore, MD 21205,

Defendants.

Case No. 1:23-cv-1826

CLASS ACTION COMPLAINT

JURY DEMAND

Plaintiff Pamela Hunter ("Plaintiff") brings this class action against Johns Hopkins The Johns Hopkins University and The Johns Hopkins Health System Corporation (collectively, "Johns Hopkins") for their failure to properly secure and safeguard Plaintiff's and Class Members' protected health information and personally identifiable information stored within Johns Hopkins's information network.

## INTRODUCTION

1. Johns Hopkins is a research and teaching hospital and associated health care

system.

2. Johns Hopkins acquired, collected, and stored Plaintiff's and Class Members' PHI/PII and/or financial information.

3. At all relevant times, Johns Hopkins knew or should have known that Plaintiff and Class Members would use Johns Hopkins's services to store and/or share sensitive data, including highly confidential PHI/PII.

4. On no later than May 31, 2023, upon information and belief, unauthorized third-party cybercriminals gained access to Plaintiff's and Class Members' PHI/PII and financial information as hosted with Johns Hopkins, with the intent of engaging in the misuse of the PII and financial information, including marketing and selling Plaintiff's and Class Members' PHI/PII.

5. The total number of individuals who have had their data exposed due to Johns Hopkins's failure to implement appropriate security safeguards is unknown at this time but is estimated to be in the tens/hundreds of thousands based on Johns Hopkins's clientele.

6. Personal health information ("PHI") is a category of information that refers to an individual's medical records and history, which is protected under the Health Insurance Portability and Accountability Act ("HIPAA"), which may include test results, procedure descriptions, diagnoses, personal or family medical histories and data points applied to a set of demographic information for a particular patient.

7. Personally identifiable information ("PII") generally incorporates information that can be used to distinguish or trace an individual's identity and is generally defined to include certain identifiers that do not on their face name an individual but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security

numbers, passport numbers, driver's license numbers, financial account numbers).

8. The vulnerable and potentially exposed data at issue of Plaintiff and the Class stored on Johns Hopkins's information network includes, without limitation, names, medical record numbers, addresses, dates of birth, Social Security numbers, and locations and dates of service related to upcoming appointments that require anesthesia.

9. Johns Hopkins disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiff's and Class Members' PHI/PII was safeguarded, failing to take available steps to prevent unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use.

10. As a result, the PHI/PII of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party—an undoubtedly nefarious third party that seeks to profit off this disclosure by defrauding Plaintiff and Class Members in the future.

11. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they are thus entitled to injunctive and other equitable relief.

## JURISDICTION AND VENUE

12. Jurisdiction is proper in this Court under 28 U.S.C. §1332 (diversity jurisdiction). Specifically, this Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action where the amount in controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one class member is a citizen of a state different from

Johns Hopkins.

13. Supplemental jurisdiction to adjudicate issues pertaining to state law is proper in this Court under 28 U.S.C. §1367.

14. Johns Hopkins is headquartered and routinely conducts business in the State where this district is located, has sufficient minimum contacts in this State, and has intentionally availed itself of this jurisdiction by marketing and selling products and services and by accepting and processing payments for those products and services within this State.

15. Venue is proper in this Court under 28 U.S.C. § 1391 because a substantial part of the events that gave rise to Plaintiff's claims occurred within this District, and Johns Hopkins does business in this Judicial District.

## THE PARTIES

**Plaintiff Pamela Hunter**

16. Plaintiff Pamela Hunter is an adult individual and, at all relevant times herein, a resident and citizen of Maryland, residing in Middle River, Maryland. Plaintiff is a victim of the Data Breach.

17. Plaintiff was a client of Johns Hopkins, and their information was stored with Johns Hopkins due to their dealings with Johns Hopkins.

18. As required to obtain services from Johns Hopkins, Plaintiff provided Johns Hopkins with highly sensitive personal, financial, health, and insurance information, who then possessed and controlled it.

19. As a result, Plaintiff's information was among the data accessed by an unauthorized third party in the Data Breach.

20. At all times herein relevant, Plaintiff is and was a member of each of the Classes.

21. Plaintiff received a letter from Johns Hopkins, dated June 24, 2023, stating that their PHI/PII and/or financial information was involved in the Data Breach (the "Notice").

22. Plaintiff was unaware of the Data Breach—or even that Johns Hopkins had possession of their data until receiving that letter.

23. As a result, Plaintiff was injured in the form of lost time dealing with the consequences of the Data Breach, which included and continues to include: time spent verifying the legitimacy and impact of the Data Breach; time spent exploring credit monitoring and identity theft insurance options; time spent self- monitoring his accounts with heightened scrutiny and time spent seeking legal counsel regarding their options for remedying and/or mitigating the effects of the Data Breach.

24. Plaintiff was also injured by the material risk to future harm she suffers based on Johns Hopkins's breach; this risk is imminent and substantial because Plaintiff's data has been exposed in the breach, the data involved, including Social Security numbers and healthcare information, is highly sensitive and presents a high risk of identity theft or fraud; and it is likely, given Johns Hopkins's clientele, that some of the Class's information that has been exposed has already been misused.

25. Plaintiff suffered actual injury in the form of damages to and diminution in the value of their PHI/PII—a condition of intangible property that they entrusted to Johns Hopkins, which was compromised in and as a result of the Data Breach.

26. Plaintiff, as a result of the Data Breach, has increased anxiety for their loss of privacy and anxiety over the impact of cybercriminals accessing, using, and selling their PHI/PII and/or financial information.

27. Plaintiff has suffered imminent and impending injury arising from the

substantially increased risk of fraud, identity theft, and misuse resulting from their PHI/PII and financial information, in combination with their name, being placed in the hands of unauthorized third parties/criminals.

28. Plaintiff has a continuing interest in ensuring that their PHI/PII and financial information, which, upon information and belief, remains backed up in Johns Hopkins's possession, is protected and safeguarded from future breaches.

**Defendants The Johns Hopkins University and The Johns Hopkins Health System Corporation**

29. Defendant The Johns Hopkins University is a research university and Maryland corporation located at 3400 N. Charles Street, Baltimore, MD 21218.

30. Defendant The Johns Hopkins Health System Corporation is a Maryland corporation with its principal place of business at 600 N. Wolfe Street, Baltimore, MD 21205.

31. The true names and capacities of persons or entities, whether individual, corporate, associate or otherwise, who may be responsible for some of the claims alleged here are currently unknown to Plaintiff.

32. Plaintiff will seek leave of court to amend this Complaint to reflect the true names and capacities of the responsible parties when their identities become known.

## CLASS ACTION ALLEGATIONS

33. Plaintiff brings this action pursuant to the provisions of Rules 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure on behalf of themself and the following classes/subclass(es) (collectively, the "Class"):

**Nationwide Class:**

All individuals within the United States of America whose PHI/PII and/or

financial information was exposed to unauthorized third parties as a result of the data breach experienced by Johns Hopkins on May 31, 2023.

**Maryland Subclass:**

All individuals within the State of Maryland whose PII/PHI was stored by Johns Hopkins and/or was exposed to unauthorized third parties as a result of the data breach experienced by Johns Hopkins on May 31, 2023.

34. Excluded from the Classes are the following individuals and/or entities: Johns Hopkins and Johns Hopkins's parents, subsidiaries, affiliates, officers and directors, and any entity in which Johns Hopkins has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to its departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as its immediate family members.

35. Plaintiff reserves the right to amend the above definitions or to propose subclasses in subsequent pleadings and motions for class certification.

36. This action has been brought and may properly be maintained as a class action under Federal Rule of Civil Procedure Rule 23 because there is a well-defined community of interest in the litigation, and membership in the proposed classes is easily ascertainable.

37. Numerosity: A class action is the only available method for the fair and efficient adjudication of this controversy, as the members of the Plaintiff Classes (which Plaintiff is informed and believes, and on that basis, alleges that the total number of persons is in the hundreds of thousands of individuals and can be determined analysis of Johns Hopkins's records) are so numerous that joinder of all members is impractical, if not impossible.

38. Commonality: Plaintiff and the Class Members share a community of interests in that there are numerous common questions and issues of fact and law which predominate

over any questions and issues solely affecting individual members, including, but not necessarily limited to:

a. Whether Johns Hopkins had a legal duty to Plaintiff and the Classes to exercise due care in collecting, storing, using, and/or safeguarding their PHI/PII;

b. Whether Johns Hopkins knew or should have known of the susceptibility of its data security systems to a data breach;

c. Whether Johns Hopkins's security procedures and practices to protect its systems were reasonable in light of the measures recommended by data security experts;

d. Whether Johns Hopkins's failure to implement adequate data security measures allowed the Data Breach to occur;

e. Whether Johns Hopkins failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

f. Whether Johns Hopkins adequately, promptly, and accurately informed Plaintiff and Class Members that their PHI/PII had been compromised;

g. How and when Johns Hopkins actually learned of the Data Breach;

h. Whether Johns Hopkins's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of the PHI/PII of Plaintiff and Class Members;

i. Whether Johns Hopkins adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Johns Hopkins engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PHI/PII of Plaintiff and Class Members;

k. Whether Plaintiff and Class Members are entitled to actual and/or statutory damages and/or whether injunctive, corrective, and/or declaratory relief and/or accounting is/are appropriate as a result of Johns Hopkins's wrongful conduct; and

l. Whether Plaintiff and Class Members are entitled to restitution as a result of Johns Hopkins's wrongful conduct.

39. Typicality: Plaintiff's claims are typical of the claims of the Plaintiff Classes. Plaintiff and all members of the Plaintiff Classes sustained damages arising out of and caused by Johns Hopkins's common course of conduct in violation of law, as alleged herein.

40. Adequacy of Representation: Plaintiff in this class action is an adequate representative of each of the Plaintiff Classes in that the Plaintiff has the same interest in the litigation of this case as the Class Members, is committed to the vigorous prosecution of this case, and has retained competent counsel who is experienced in conducting litigation of this nature.

41. Plaintiff is not subject to any individual defenses unique from those conceivably applicable to other Class Members or the classes in its entirety. Plaintiff anticipates no management difficulties in this litigation.

42. Superiority of Class Action: Since the damages suffered by individual Class Members, while not inconsequential, may be relatively small, the expense and burden of individual litigation by each member make or may make it impractical for members of the

Plaintiff Classes to seek redress individually for the wrongful conduct alleged herein. Should separate actions be brought or required to be brought by each member of the Plaintiff Classes, the resulting multiplicity of lawsuits would cause undue hardship and expense for the Court and the litigants.

43. The prosecution of separate actions would also create a risk of inconsistent rulings, which might be dispositive of the interests of the Class Members who are not parties to the adjudications and/or may substantially impede their ability to protect their interests adequately.

44. This class action is also appropriate for certification because Johns Hopkins has acted or refused to act on grounds generally applicable to Class Members, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class in its entirety.

45. Johns Hopkins's policies and practices challenged herein apply to and affect Class Members uniformly, and Plaintiff's challenge of these policies and practices hinges on Johns Hopkins's conduct with respect to the Class in its entirety, not on facts or law applicable only to Plaintiff.

46. Unless a Class-wide injunction is issued, Johns Hopkins may continue failing to properly secure the PHI/PII and/or financial information of Class Members, and Johns Hopkins may continue to act unlawfully as set forth in this Complaint.

47. Further, Johns Hopkins has acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

## COMMON FACTUAL ALLEGATIONS

### Johns Hopkins's Failed Response to the Breach

48. Not until after months it claims to have discovered the Data Breach did Johns Hopkins begin sending the Notice to persons whose PHI/PII and/or financial information Johns Hopkins confirmed was potentially compromised as a result of the Data Breach.

49. The Notice included *inter alia*, basic details of the Data Breach, Johns Hopkins's recommended next steps, and Johns Hopkins's claims that it had learned of the Data Breach on May 31, 2023, and completed a review thereafter.

50. Upon information and belief, the unauthorized third-party cybercriminals gained access to Plaintiff's and Class Members' PHI/PII and financial information with the intent of engaging in the misuse of the PHI/PII and financial information, including marketing and selling Plaintiff's and Class Members' PHI/PII.

51. Johns Hopkins had and continues to have obligations created by HIPAA, applicable federal and state law as set forth herein, reasonable industry standards, common law, and its own assurances and representations to keep Plaintiff's and Class Members' PHI/PII confidential and to protect such PHI/PII from unauthorized access.

52. Plaintiff and Class Members were required to provide their PHI/PII and financial information to Johns Hopkins as a condition of their employment, and as part of providing employment and providing healthcare services, Johns Hopkins created, collected, and stored Plaintiff and Class Members with the reasonable expectation and mutual understanding that Johns Hopkins would comply with its obligations to keep such information confidential and secure from unauthorized access.

53. Despite this, Plaintiff and the Class Members remain, even today, in the dark

regarding what data was stolen, the particular malware used, and what steps are being taken to secure their PHI/PII and financial information going forward.

54. Plaintiff and Class Members are, thus, left to speculate as to where their PHI/PII ended up, who has used it, and for what potentially nefarious purposes, and are left to further speculate as to the full impact of the Data Breach and how exactly Johns Hopkins intends to enhance its information security systems and monitoring capabilities to prevent further breaches.

55. Unauthorized individuals can now easily access the PHI/PII and/or financial information of Plaintiff and Class Members.

**Johns Hopkins Collected/Stored Class Members' PHI/PII and Financial Information**

56. Johns Hopkins acquired, collected, stored, and assured reasonable security over Plaintiff's and Class Members' PHI/PII and financial information.

57. As a condition of its relationships with Plaintiff and Class Members, Johns Hopkins required that Plaintiff and Class Members entrust Johns Hopkins with highly sensitive and confidential PHI/PII and financial information.

58. Johns Hopkins, in turn, stored that information in the part of Johns Hopkins's system that was ultimately affected by the Data Breach.

59. By obtaining, collecting, and storing Plaintiff's and Class Members' PHI/PII and financial information, Johns Hopkins assumed legal and equitable duties and knew or should have known that they were thereafter responsible for protecting Plaintiff's and Class Members' PHI/PII and financial information from unauthorized disclosure.

60. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PHI/PII and financial information.

61. Plaintiff and Class Members relied on Johns Hopkins to keep their PHI/PII and financial information confidential and securely maintained, to use this information for business and healthcare purposes only, and to make only authorized disclosures of this information.

62. Johns Hopkins could have prevented the Data Breach, which began no later than May 31, 2023, by adequately securing and encrypting and/or more securely encrypting its servers generally and Plaintiff's and Class Members' PHI/PII and financial information.

63. Johns Hopkins's negligence in safeguarding Plaintiff's and Class Members' PHI/PII and financial information is exacerbated by repeated warnings and alerts directed to protecting and securing sensitive data, as evidenced by the trending data breach attacks in recent years.

64. Yet, despite the prevalence of public announcements of data breaches and data security compromises, Johns Hopkins failed to take appropriate steps to protect Plaintiff's and Class Members' PHI/PII and financial information from being compromised.

**Johns Hopkins Had an Obligation to Protect the Stolen Information**

65. Johns Hopkins's failure to adequately secure Plaintiff's and Class Members' sensitive data breaches duties it owes Plaintiff and Class Members under statutory and common law. Under HIPAA, health insurance providers have an affirmative duty to keep patients' Protected Health Information private. As a covered entity, Johns Hopkins has a statutory duty under HIPAA and other federal and state statutes to safeguard Plaintiff's and Class Members' data. Moreover, Plaintiff and Class Members surrendered their highly sensitive personal data to Johns Hopkins under the implied condition that Johns Hopkins would keep it private and secure. Accordingly, Johns Hopkins also has an implied duty to safeguard their data, independent of

any statute.

66. Because Johns Hopkins is covered by HIPAA (45 C.F.R. § 160.102), it is required to comply with the HIPAA Privacy Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

67. HIPAA's Privacy Rule or Standards for Privacy of Individually Identifiable Health Information establishes national standards for protecting health information.

68. HIPAA's Privacy Rule or Security Standards for the Protection of Electronic Protected Health Information establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

69. HIPAA requires Johns Hopkins to "comply with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronically protected health information." 45 C.F.R. § 164.302.

70. "Electronic protected health information" is "individually identifiable health information … that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

71. HIPAA's Security Rule requires Johns Hopkins to do the following:

a. Ensure the confidentiality, integrity, and availability of all electronically protected health information the covered entity or business associate creates, receives, maintains, or transmits;

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by its workforce.

72. HIPAA also requires Johns Hopkins to "review and modify the security measures implemented … as needed to continue provision of reasonable and appropriate protection of electronically protected health information" under 45 C.F.R. § 164.306(e), and to "[i]mplement technical policies and procedures for electronic information systems that maintain electronically protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

73. Moreover, the HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, requires Johns Hopkins to provide notice of the Data Breach to each affected individual "without unreasonable delay and in no case later than 60 days following the discovery of the breach."

74. Johns Hopkins was also prohibited by the Federal Trade Commission Act (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce."[1]

75. In addition to its obligations under federal and state laws, Johns Hopkins owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PHI/PII and financial information in Johns Hopkins's possession from being compromised, lost, stolen, accessed, and misused by

[1] The Federal Trade Commission (the "FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. See, e.g., *FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015).

unauthorized persons.

76. Johns Hopkins owed a duty to Plaintiff and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the PHI/PII and financial information of Plaintiff and Class Members.

77. Johns Hopkins owed Plaintiff and Class Members a duty to design, maintain, and test its computer systems, servers, and networks to ensure that the PHI/PII and financial information was adequately secured and protected.

78. Johns Hopkins owed Plaintiff and Class Members a duty to create and implement reasonable data security practices and procedures to protect the PHI/PII and financial information in its possession, including not sharing information with other entities who maintained sub-standard data security systems.

79. Johns Hopkins owed a duty to Plaintiff and Class Members to implement processes that would immediately detect a breach in its data security systems in a timely manner.

80. Johns Hopkins owed a duty to Plaintiff and Class Members to act upon data security warnings and alerts in a timely fashion.

81. Johns Hopkins owed a duty to Plaintiff and Class Members to disclose if its computer systems and data security practices were inadequate to safeguard individuals' PHI/PII and/or financial information from theft because such an inadequacy would be a material fact in the decision to entrust this PHI/PII and/or financial information to Johns Hopkins.

82. Johns Hopkins owed a duty of care to Plaintiff and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

83. Johns Hopkins owed a duty to Plaintiff and Class Members to encrypt and/or

more reliably encrypt Plaintiff's and Class Members' PHI/PII and financial information and monitor user behavior and activity to identify possible threats.

**Value of the Relevant Sensitive Information**

84. PHI/PII and financial information are valuable commodities for which a "cyber black market" exists in which criminals openly post stolen payment card numbers, Social Security numbers, and other personal information on several underground internet websites.

85. Numerous sources cite dark web pricing for stolen identity credentials; for example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200[2]; Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web[3]; and other sources report that criminals can also purchase access to entire company data breaches from $999 to $4,995.[4]

86. Identity thieves can use PHI/PII and financial information, such as that of Plaintiff and Class Members, which Johns Hopkins failed to keep secure, to perpetrate a variety of crimes that harm victims—for instance, identity thieves may commit various types of government fraud such as immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, using the victim's information to obtain government benefits, or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

---

[2] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed July 5, 2023).

[3] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed July 5, 2023).

[4] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed July 5, 2023).

87. There may be a time lag between when harm occurs versus when it is discovered, and also between when PHI/PII and/or financial information is stolen and when it is used: according to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data might be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[5]

88. Here, Johns Hopkins knew of the importance of safeguarding PHI/PII and financial information and of the foreseeable consequences that would occur if Plaintiff's and Class Members' PHI/PII and financial information were stolen, including the significant costs that would be placed on Plaintiff and Class Members as a result of a breach of this magnitude.

89. As detailed above, Johns Hopkins is a large, sophisticated organization with the resources to deploy robust cybersecurity protocols. It knew or should have known, that the development and use of such protocols were necessary to fulfill its statutory and common law duties to Plaintiff and Class Members. Therefore, its failure to do so is intentional, willful, reckless, and/or grossly negligent.

90. Johns Hopkins disregarded the rights of Plaintiff and Class Members by, *inter alia*, (i) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that its network servers were protected against unauthorized intrusions; (ii) failing to disclose that they did not have adequately robust security protocols and training practices in place to adequately safeguard Plaintiff's and Class Members' PHI/PII and/or

[5] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* http://www.gao.gov/new.items/d07737.pdf (last accessed July 5, 2023).

financial information; (iii) failing to take standard and reasonably available steps to prevent the Data Breach; (iv) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (v) failing to provide Plaintiff and Class Members prompt and accurate notice of the Data Breach.

## CLAIMS FOR RELIEF

### COUNT ONE
**Negligence**
**(On behalf of the Nationwide Class and the Maryland Subclass)**

91. Plaintiff realleges and reincorporates every allegation set forth in the preceding paragraphs as though fully set forth herein.

92. At all times herein relevant, Johns Hopkins owed Plaintiff and Class Members a duty of care, *inter alia*, to act with reasonable care to secure and safeguard their PHI/PII and financial information and to use commercially reasonable methods to do so. Johns Hopkins took on this obligation upon accepting and storing the PHI/PII and financial information of Plaintiff and Class Members in its computer systems and networks.

93. Among these duties, Johns Hopkins was expected:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PHI/PII and financial information in its possession;

b. to protect Plaintiff's and Class Members' PHI/PII and financial information using reasonable and adequate security procedures and systems that were/are compliant with industry-standard practices;

c. to implement processes to detect the Data Breach quickly and to act on warnings about data breaches timely; and

d. to promptly notify Plaintiff and Class Members of any data breach, security incident, or intrusion that affected or may have affected their PHI/PII and financial information.

94. Johns Hopkins knew that the PHI/PII and financial information was private and confidential and should be protected as private and confidential and, thus, Johns Hopkins owed a duty of care not to subject Plaintiff and Class Members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

95. Johns Hopkins knew or should have known, of the risks inherent in collecting and storing PHI/PII and financial information, the vulnerabilities of its data security systems, and the importance of adequate security.

96. Johns Hopkins knew about numerous well-publicized data breaches.

97. Johns Hopkins knew or should have known, that its data systems and networks did not adequately safeguard Plaintiff's and Class Members' PHI/PII and financial information.

98. Only Johns Hopkins was in the position to ensure that its systems and protocols were sufficient to protect the PHI/PII and financial information that Plaintiff and Class Members had entrusted to it.

99. Johns Hopkins breached its duties to Plaintiff and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard their PHI/PII and financial information.

100. Because Johns Hopkins knew that a breach of its systems could damage thousands of individuals, including Plaintiff and Class Members, Johns Hopkins had a duty to adequately protect its data systems and the PHI/PII and financial information contained therein.

101. Plaintiff's and Class Members' willingness to entrust Johns Hopkins with their

PHI/PII and financial information was predicated on the understanding that Johns Hopkins would take adequate security precautions.

102. Moreover, only Johns Hopkins could protect its systems, and the PHI/PII and financial information is stored on them from attack. Thus, Johns Hopkins had a special relationship with Plaintiff and Class Members.

103. Johns Hopkins also had independent duties under state and federal laws that required Johns Hopkins to reasonably safeguard Plaintiff's and Class Members' PHI/PII and financial information and promptly notify them about the Data Breach. These "independent duties" are untethered to any contract between Johns Hopkins, Plaintiff, and/or the remaining Class Members.

104. Johns Hopkins breached its general duty of care to Plaintiff and Class Members in, but not necessarily limited to, the following ways:

a. by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard the PHI/PII and financial information of Plaintiff and Class Members;

b. by failing to timely and accurately disclose that Plaintiff's and Class Members' PHI/PII and financial information had been improperly acquired or accessed;

c. by failing to adequately protect and safeguard the PHI/PII and financial information by knowingly disregarding standard information security principles, despite obvious risks and by allowing unmonitored and unrestricted access to unsecured PHI/PII and financial information;

d. by failing to provide adequate supervision and oversight of the PHI/PII

and financial information with which it was and is entrusted, despite the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather PHI/PII and financial information of Plaintiff and Class Members, misuse the PHI/PII and intentionally disclose it to others without consent.

e. by failing to adequately train its employees not to store PHI/PII and financial information longer than absolutely necessary;

f. by failing to consistently enforce security policies aimed at protecting Plaintiff's and the Class Members' PHI/PII and financial information;

g. by failing to implement processes to detect data breaches, security incidents, or intrusions quickly; and

h. by failing to encrypt Plaintiff's and Class Members' PHI/PII and financial information and monitor user behavior and activity to identify possible threats.

105. Johns Hopkins's willful failure to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

106. As a proximate and foreseeable result of Johns Hopkins's grossly negligent conduct, Plaintiff and Class Members have suffered damages and are at imminent risk of additional harm and damages.

107. The law further imposes an affirmative duty on Johns Hopkins to timely disclose the unauthorized access and theft of the PHI/PII and financial information to Plaintiff and Class Members so that they could and/or still can take appropriate measures to mitigate damages, protect against adverse consequences and thwart future misuse of their PHI/PII and financial

information.

108. Johns Hopkins breached its duty to notify Plaintiff and Class Members of the unauthorized access by waiting months after learning of the Data Breach to notify Plaintiff and Class Members and then by failing and continuing to fail to provide Plaintiff and Class Members sufficient information regarding the breach.

109. To date, Johns Hopkins has not provided sufficient information to Plaintiff and Class Members regarding the extent of the unauthorized access and continues to breach its disclosure obligations to Plaintiff and Class Members.

110. Further, through its failure to provide timely and clear notification of the Data Breach to Plaintiff and Class Members, Johns Hopkins prevented Plaintiff and Class Members from taking meaningful, proactive steps to secure their PHI/PII and financial information and to access their medical records and histories.

111. There is a close causal connection between Johns Hopkins's failure to implement security measures to protect the PHI/PII and financial information of Plaintiff and Class Members and the harm suffered, or risk of imminent harm suffered by Plaintiff and Class Members.

112. Plaintiff's and Class Members' PHI/PII and financial information was accessed as the proximate result of Johns Hopkins's failure to exercise reasonable care in safeguarding such PHI/PII and financial information by adopting, implementing, and maintaining appropriate security measures.

113. Johns Hopkins's wrongful actions, inactions, and omissions constituted (and continue to constitute) common law negligence.

114. The damages Plaintiff and Class Members have suffered (as alleged above) and

will suffer were and are the direct and proximate result of Johns Hopkins's grossly negligent conduct.

115. As a direct and proximate result of Johns Hopkins's negligence and negligence *per se*, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PHI/PII and financial information is used; (iii) the compromise, publication, and/or theft of their PHI/PII and financial information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PHI/PII and financial information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to, efforts spent researching how to prevent, detect, contest, and recover from embarrassment and identity theft; (vi) lost continuity in relation to their healthcare; (vii) the continued risk to their PHI/PII and financial information, which may remain in Johns Hopkins's possession and is subject to further unauthorized disclosures so long as Johns Hopkins fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PHI/PII and financial information in its continued possession; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PHI/PII and financial information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

116. As a direct and proximate result of Johns Hopkins's negligence and negligence *per se*, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

117. Additionally, as a direct and proximate result of Johns Hopkins's negligence, Plaintiff and Class Members have suffered and will suffer the continued risks of exposure of their PHI/PII and financial information, which remain in Johns Hopkins's possession and are subject to further unauthorized disclosures so long as Johns Hopkins fails to undertake appropriate and adequate measures to protect the PHI/PII and financial information in its continued possession.

**COUNT TWO**
**Breach of Implied Contract**
**(On behalf of the Nationwide Class and the Maryland Subclass)**

118. Plaintiff realleges and reincorporates every allegation set forth in the preceding paragraphs as though fully set forth herein.

119. Through its course of conduct, Johns Hopkins, Plaintiff, and Class Members entered into implied contracts for Johns Hopkins to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' PHI/PII and financial information.

120. Johns Hopkins required Plaintiff and Class Members to provide and entrust their PHI/PII and financial information as a condition of obtaining Johns Hopkins's services.

121. Johns Hopkins solicited and invited Plaintiff and Class Members to provide their PHI/PII and financial information as part of Johns Hopkins's regular business practices.

122. Plaintiff and Class Members accepted Johns Hopkins's offers and provided their PHI/PII and financial information to Johns Hopkins.

123. As a condition of being direct patients of clients of Johns Hopkins, Plaintiff, and Class Members provided and entrusted their PHI/PII and financial information to Johns Hopkins.

124. In so doing, Plaintiff and Class Members entered into implied contracts with Johns Hopkins by which Johns Hopkins agreed to safeguard and protect such non-public information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and Class Members if their data had been breached and compromised or stolen.

125. A meeting of the minds occurred when Plaintiff and Class Members agreed to and did, provide their PHI/PII and financial information to Johns Hopkins, in exchange for, amongst other things, the protection of their PHI/PII and financial information.

126. Plaintiff and Class Members fully performed their obligations under the implied contracts with Johns Hopkins.

127. Johns Hopkins breached its implied contracts with Plaintiff and Class Members by failing to safeguard and protect their PHI/PII and financial information and by failing to provide timely and accurate notice to them that their PHI/PII and financial information was compromised as a result of the Data Breach.

128. As a direct and proximate result of Johns Hopkins's above-described breach of implied contract, Plaintiff and Class Members have suffered (and will continue to suffer) (a) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; (b) actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; (c) loss of the confidentiality of the stolen confidential data; (d) the illegal sale of the compromised data on the dark web; (e) lost work time; and (f) other economic and non-economic harm.

## COUNT THREE
**Breach of the Implied Covenant of Good Faith and Fair Dealing**
**(On behalf of the Nationwide Class and the Maryland Subclass)**

129. Plaintiff realleges and reincorporates every allegation set forth in the preceding

paragraphs as though fully set forth herein.

130. Every contract in this State has an implied covenant of good faith and fair dealing, which is an independent duty and may be breached even when there is no breach of a contract's actual and/or express terms.

131. Plaintiff and Class Members have complied with and performed all conditions of their contracts with Johns Hopkins.

132. Johns Hopkins breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices to safeguard PHI/PII and financial information, failing to timely and accurately disclose the Data Breach to Plaintiff and Class Members and continued acceptance of PHI/PII and financial information and storage of other personal information after Johns Hopkins knew, or should have known, of the security vulnerabilities of the systems that were exploited in the Data Breach.

133. Johns Hopkins acted in bad faith and/or with malicious motive in denying Plaintiff and Class Members the full benefit of their bargains as originally intended by the parties, thereby causing them injury in an amount to be determined at trial.

**COUNT FOUR**
**Unjust Enrichment**
**(On behalf of the Nationwide Class and the Maryland Subclass)**

134. Plaintiff realleges and reincorporates every allegation set forth in the preceding paragraphs as though fully set forth herein.

135. By its wrongful acts and omissions described herein, Johns Hopkins has obtained a benefit by unduly taking advantage of Plaintiff and Class Members.

136. Johns Hopkins, prior to and at the time Plaintiff and Class Members entrusted their PHI/PII and financial information to Johns Hopkins for the purpose of obtaining health services, caused Plaintiff and Class Members to reasonably believe that Johns Hopkins would

keep such PHI/PII and financial information secure.

137. Johns Hopkins was aware or should have been aware, that reasonable patients and consumers would have wanted their PHI/PII and financial information kept secure and would not have contracted with Johns Hopkins, directly or indirectly, had they known that Johns Hopkins's information systems were sub-standard for that purpose.

138. Johns Hopkins was also aware that if the substandard condition of and vulnerabilities in its information systems were disclosed, it would negatively affect Plaintiff's and Class Members' decisions to seek services therefrom.

139. Johns Hopkins failed to disclose facts about its substandard information systems, defects, and vulnerabilities therein before Plaintiff and Class Members decided to make purchases, engage in commerce therewith, and seek services or information.

140. Instead, Johns Hopkins suppressed and concealed such information. By concealing and suppressing that information, Johns Hopkins denied Plaintiff and Class Members the ability to make a rational and informed purchasing and healthcare decision and took undue advantage of Plaintiff and Class Members.

141. Johns Hopkins was unjustly enriched at the expense of Plaintiff and Class Members, as Johns Hopkins received profits, benefits, and compensation, in part, at the expense of Plaintiff and Class Members; however, Plaintiff and Class Members did not receive the benefit of their bargain because they paid for products and/or health care services that did not satisfy the purposes for which they bought/sought them.

142. Since Johns Hopkins's profits, benefits, and other compensation were obtained improperly, Johns Hopkins is not legally or equitably entitled to retain any of the benefits, compensation, or profits it realized from these transactions.

143. Plaintiff and Class Members seek an Order of this Court requiring Johns Hopkins to refund, disgorge, and pay as restitution any profits, benefits, and other compensation obtained by Johns Hopkins from its wrongful conduct and/or the establishment of a constructive trust from which Plaintiff and Class Members may seek restitution.

## PRAYER FOR RELIEF

**WHEREFORE,** Plaintiff, on behalf of themself and each member of the proposed National Class and the Maryland Subclass, respectfully request that the Court enter judgment in their favor and for the following specific relief against Johns Hopkins as follows:

1. That the Court declare, adjudge, and decree that this action is a proper class action and certify each of the proposed classes and/or any other appropriate subclasses under F.R.C.P. Rule 23 (b)(1), (b)(2), and/or (b)(3), including the appointment of Plaintiff's counsel as Class Counsel;

2. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

3. That the Court enjoin Johns Hopkins, ordering them to cease unlawful activities;

4. For equitable relief enjoining Johns Hopkins from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PHI/PII and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and Class Members;

5. For injunctive relief requested by Plaintiff, including but not limited to injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an Order:

a. prohibiting Johns Hopkins from engaging in the wrongful and unlawful

acts described herein;

b. requiring Johns Hopkins to protect, including through encryption, all data collected through the course of business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

c. requiring Johns Hopkins to delete and purge the PHI/PII of Plaintiff and Class Members unless Johns Hopkins can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

d. requiring Johns Hopkins to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiff's and Class Members' PHI/PII;

e. requiring Johns Hopkins to engage independent third-party security auditors and internal personnel to run automated security monitoring, simulated attacks, penetration tests, and audits on Johns Hopkins's systems periodically;

f. prohibiting Johns Hopkins from maintaining Plaintiff's and Class Members' PHI/PII on a cloud-based database;

g. requiring Johns Hopkins to segment data by creating firewalls and access controls so that, if one area of Johns Hopkins's network is compromised, hackers cannot gain access to other portions of Johns Hopkins's systems;

h. requiring Johns Hopkins to conduct regular database scanning and securing checks;

i. requiring Johns Hopkins to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PHI/PII, as well as protecting the PHI/PII of Plaintiff and Class Members;

j. requiring Johns Hopkins to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Johns Hopkins's policies, programs, and systems for protecting personal identifying information;

k. requiring Johns Hopkins to implement, maintain, review, and revise as necessary a threat management program to monitor Johns Hopkins's networks for internal and external threats appropriately and assess whether monitoring tools are properly configured, tested, and updated; and

l. requiring Johns Hopkins to meaningfully educate all Class Members about the threats they face due to the loss of their confidential personal identifying information to third parties and the steps affected individuals must take to protect themselves.

6. For prejudgment interest on all amounts awarded at the prevailing legal rate;

7. For an award of attorney's fees, costs, and litigation expenses, as allowed by law; and

8. For all other Orders, findings, and determinations identified and sought in

this Complaint.

**JURY DEMAND**

Plaintiff, individually and on behalf of the Plaintiff Class(es) and/or Subclass(es), hereby demands a trial by jury for all issues triable by jury.

Dated: July 7, 2023

Respectfully submitted,

By: */s/ Courtney L. Weiner*

Courtney L. Weiner
1629 K Street, NW, Suite 300
Washington, DC 20006
T: (202) 827-9980
cw@courtneyweinerlaw.com

**LAUKAITIS LAW LLC**
Kevin Laukaitis (PA ID 321670)*
954 Avenida Ponce De Leon
Suite 205, #10518
San Juan, PR 00907
T: (215) 789-4462
klaukaitis@laukaitislaw.com

**Pro Hac Vice admission forthcoming*

Attorneys for Plaintiff(s) and the Plaintiff Class(es)